AARMS Vol. 19, No. 1 (2020) 65–81.

10.32565/aarms.2020.1.6

Opportunities of Darknet Operations in Cyber Warfare: Examining its Functions and Presence in the University Environment

Ferenc KOCZKA[1]

Regarding the Internet, individuals expect anonymity and confidentiality, but the authorities expect as much traceability as possible. Individuals are provided with encryption procedures used in internet communication, supported by more and more efficient devices and applications. For law enforcement, the publicity of these procedures could be a serious problem. However, in addition to a well-functioning technical background, conscious use of tools is required to maintain anonymity. In this article I present the necessary techniques to achieve this goal, their operational principles, scopes and points that may enable the technology to be compromised. In the second part of this article, the partial results of my research will be presented, which measures the presence and activity of the darknet; it can provide a basis for carrying out similar investigations and can help develop the protection process.

Keywords: *darknet, VPN, TOR, onion routing, electronic warfare.*

Introduction

The supervision and military use of cyberspace is necessary not only in defence, but also in the achievement of information superiority, and is in the primary interest of all countries. This fact has been recognised by the military leadership of many countries and they elaborated, at least partially, some kind of strategy for warfare in cyberspace. In each of these strategies, there is a clear integrative effort to handle the potential and the threats of cyberspace in line with traditional military infrastructures and activities. The supervision and control of cyberspace is an essential task, but given the previously unimaginable amount of data and quite varied communication methods, this requires a fundamentally new approach.

Previously, tools and procedures developed for military purposes in civilian life were typically not available, at most only with a long delay. However, with regard to cyberspace, this is not the case: there are public procedures for encrypting, obfuscating and concealing data and preserving confidentiality, against which the major military powers do not have an effective means of defence.

[1] IT director at Eszterházy Károly University; e-mail: koczka.ferenc@uni-eszterhazy.hu; ORCID: https://orcid.org/0000-0002-7541-6495

The darknet may play a special role in certain areas of information operations. Although the darknet is based on military development, its potential can be used against anyone, including its creator. The purpose of this article is to review darknet, to raise awareness of the military application capabilities, functionality and scope of darknet, and to present the results of a measurement that examined the presence and use of darknet. In doing so, I use a combined research paradigm. First, by means of a deductive research strategy, I review the main characteristics of darknet, and then comes, in the context of inductive logic, the case study and the cross-sectional study. I examined a large section of domestic higher education using the logfile analysis method in Eszterházy Károly University on this issue.

Layers of the Web

With the rapid development of the Internet, the number of computers connected to the network is also growing rapidly; some sources say that in September 2019, 58% of the total population of the Earth, 4.33 billion people, had Internet access. [1] This technical opportunity brought along a number of applications that have become decisive for the daily existence of mankind and have made many previous methods or resources outdated or replaced them with new ones. The most popular service is still the web, which has become an interactive and dynamic service that combines a wide range of technologies from the initial simple and static descriptive html base. The number of websites has exploded, with approximately 1.7 billion sites operating. When writing these lines, [2] finding the necessary information and navigating them was a problem from the outset. In the early stages of the Internet, it was advisable to use various collection sites, which were later almost completely replaced by search engines[2]—the extent of their dominance is illustrated by the fact that today, when developing websites, developers need to take their expectations into account. Search engines work based on background programs (so-called bots) that continuously monitor the entire web space and collect its data into their database that is the base of searching processes. The set of websites to be visited by search bots is mainly from internet name servers,[3] which are supplemented by links found in processed web pages. Therefore, search engines are far from being able to map the entire web universe, leaving many websites invisible to them—some sources consider the number of visible websites to be 4% of the total web.

From the perspective of access, web content is classified into three different classes. Open access websites and contents that search engines find are called surface web.

Web contents that use surface web technology but are invisible to search engines are a second layer called the deep web. Invisibility can be for many reasons, including pages

[2] The first really popular search engine was Altavista (http://altavista.com), founded in 1995. Its rivals (Google, Bing, Yahoo, etc.) used much better technologies, so it was pointless to maintain it. The name has been owned by Yahoo since 2003.

[3] Name servers (DNS servers) store internet names that represent the addresses of websites. Naming is not technically indispensable, but their absence would make it difficult to access pages because, among other limitations, they could only be referenced with an IP address. Therefore, websites containing public information always have DNS names, which is an ideal starting point for search engines.

protected[4] by the password or captcha, contents available only after registration, personal accounts, private cloud storage, virtual offices, content returned based on search for each page, results of database queries and responses returned to non-http or https. Web contents that are not shown by any external links or DNS entries remain invisible for search engines. The deep web and surface web operate with the same technology and therefore do not provide anonymity to the service provider or the party that uses it. It is not ideal to display non-public content because of this, although there are exceptions.[5]

The third layer is also invisible to search engines, because its network technology is different from that used in the previous two layers, so you need specialised software to reach it. This part of the Internet, called darknet, was created for a double purpose. On the one hand, it provides anonymity to the person who browses, so that the identity of the content service server operator is hidden. On the other hand, it is to hide servers, in which darknet's infrastructure ensures that the exact location of content servers cannot be determined during their operation. The infrastructure implemented by darknet requires a software specialised for this purpose, and traditional browsers cannot be used to access web pages that are operated there.

Darknet's assessment is controversial, as the need for anonymity subsists in practice in four main areas. On the one hand, it acts as a means of avoiding network control and censorship in repressive regimes and provides anonymity to users who need to be cautious. It is also to secure sensitive data transmission, server hiding, and data leaking. Darknet's client-side anonymity feature has been used by the New York Times from 2017, the BBC from 2019, and other newspapers followed. [3, 4] In Hungary, it is used in investigative journalism to receive content in which the identity of the person who leaks the data is to be hidden. [5] China's internet restrictions are well known, but this feature also plays a great role in other countries, such as Saudi Arabia, because of restrictions and monitoring of networks. [6] In these countries, restrictions on access to web content can be circumvented using darknet,[6] so the DuckDuckGo search engine is available as an alternative to Google, as well as the alternative Facebook,[7] which already received one million visitors a month in 2016.

Darknet also provides servers with anonymity, which is also an excellent opportunity for criminals. Based on its concealment capabilities, their services can be hidden and operate with great certainty, leaving its exact location undetectable. In this part of cyberspace, all types of illegal activities can be carried out which do not require a personal presence: from trade in credit card data, drugs, ransomware and organs to the distribution of drugs, weapons, information and raw materials, all are available. Darknet protects Wikileaks documents,[8] 3D-printed weapons files, and many other areas of crime that go beyond the scope of this article. The veracity of the services that criminals provide is always doubtful, sellers are unknown in the protection of technology, and there is no possibility of a claim

---

4 Captcha is a control question that computer programs are currently unable to answer. Typical examples are hard-to-recognise texts, possibly counting tasks.

5 There are a number of websites that publish illegal—or at least questionable—content through the internet service provider that runs them on the surface web, with the ISP running them operating in one of the developed countries. For example, Satan's Temple at https://www.churchofsatan.com. The Inspire Magazine is now usually distributed on publicly accessed but hacked websites.

6 *Source:* http://3g2upl4pq6kufc4m.onion/

7 *Source:* www.facebookcorewwwi.onion/

8 WikiLeaks is available at http://suw74isz7wqzpmgu.onion

or a guarantee. There are several attempts to infect the visitor's computer, steal data, and install malware. Since the payment for illegal services is usually made in a cryptocurrency, they often try to access crypto wallets using sophisticated methods on darknet. They analyse the contents of the clipboard and try to exchange the identification code for bitcoin wallets found therein, or to publish and hijack the payment process with a modified browser which they have manipulated. [7]

The interests of national defence justifies research on the issue in order to monitor or possibly prevent the functioning of darknet and its alternatives, and to develop control and eradication options for illegal activities carried out there.

Implementation Options

There are several ways to implement anonymity and confidentiality. The Tor Browser is certainly the best-known browser for web use, which builds on the Tor protocol to hide the IP address of the browsing machine. This browser is actually a modified Firefox that connects with the target web server via the Tor network and initiates the download of the page. Tor Browser functionality can be reached with plug-ins for other browsers. From an operational point of view, I2P and FreeNet are alternatives, both of which require a combined infrastructure for service users to provide anonymity insurance.

Another solution is to channel data traffic into an encrypted channel, typically based on a VPN server. The two leading providers of VPN[9] solutions today are ExpressVPN and NordVPN.[10] When using such a service, the client traffic is transferred through one of the VPN provider's servers and transmits its requests (even twice) to service providers in the encrypted form. The request is sent to the destination server by the VPN provider's server so that they can only identify its IP address. The target server returns its response to the VPN server, which sends it back to the client. Client anonymity is guaranteed by the logging strategy provided by the VPN provider, and it is questionable whether, in critical cases, it can help authorities to establish the identity of the person requesting anonymity.

Both solutions have advantages and disadvantages, but since they can be used together, it is recommended to combine them to improve the security of anonymity.

Other methods of anonymous access also exist: the so-called on-the-go operating systems can be installed on a CD or USB drive on any machine, with only the most necessary information available to others.

Chat software that provides encrypted communications are another situation, some of which are based on central servers, while others rely on peer-to-peer relationships. Their best-known representatives are Telegram, Tox and Signal, which was considered the safest by Edward Snowden.

The range of softwares aimed at encrypted communications and user anonymisation is expanded from time to time, so that people who wish to use it can easily find another alternative when a system is compromised. However, an error in the principles or even in the implementation of a particular software easily results in a loss of confidentiality.

---

[9] *Source:* www.expressvpn.com

[10] *Source:* https://nordvpn.com

The TOR

Tor stands for *The Onion Router,* developed by United States Naval Research Laboratory (NRL) to protect government communications in the mid-1990s. The first publicly available version was released in 2002. The source code was later made free by the NRL, opening the door to a wide spread and further development. The development continued in 2006 by The Tor Project, a non-profit organisation that develops and maintains Tor today, although in 2016 the entire development team quit and their positions were replaced by others.

The Tor network is based on a system of independent Tor nodes. The basic task of such a node is to ensure the encrypted transmission of data packets flowing through it to an adjacent node, which is currently done with a 128-bit symmetrical key.

Some nodes are configured differently, so they play a prominent role: they can be used to exit the public Internet, i.e. these points provide a connection to the surface and deep internet, so they are used as exit nodes.

The Tor network is therefore based on encrypted traffic between each node, so that the order of the nodes in that relationship will only be the same during a session. This feature is performed by a single component, the Tor browser, while for alternative implementations, the browser and the component for maintaining the network can be implemented in two separate softwares. The nodes that participate in the sessions are selected by the client itself (the so-called initiator). This step queries a list[11] of guard nodes that serve as the entry points from one of the Tor directory servers,[12] then, based on this knowledge, selects the nine machines and exit points that you will use in that session.

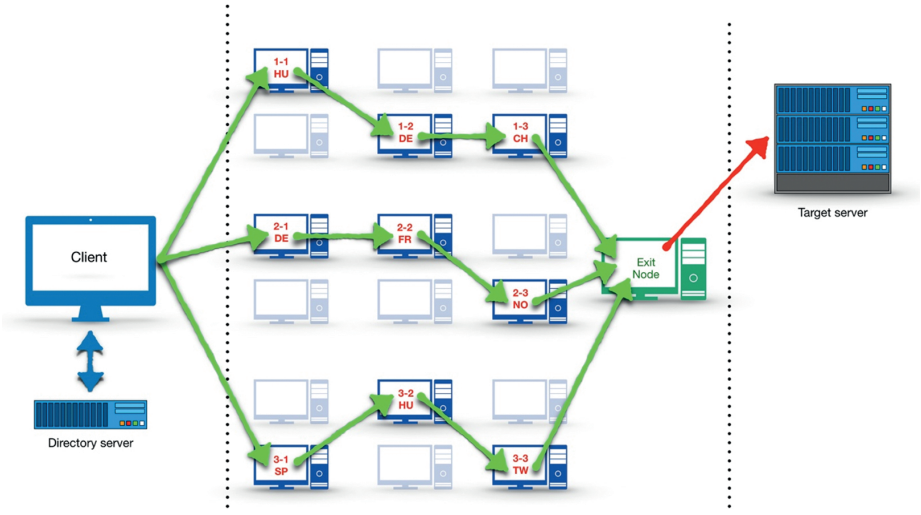

Figure 1. *How the Tor protocol works.* [Created by the author.]

[11] Their current list is available at: www.dan.me.uk/torlist/

[12] There are a number of rules when choosing nodes. On the one hand, they must be a sufficient distance apart, i.e. they must not be in the same subnet of /16. Guard nodes must be privileged nodes since they know the IP address of the client.

Tor's encryption method is different from the general method. As a first step, the initiator generates a master key to encrypt the data package that it must send over the network. After that it appends the master key to the encrypted package, then cuts the resulting package into three parts and starts them on the previously generated route (circuit). The method ensures that the master key required to decode the contents of the package is never fully present on any node. Each node encrypts the part of the subpackage that is on it over and over again, while also adding the key needed to decrypt the encryption. Thus, each of the keys used by each node is included in the transferred sub-data pack, so any node can decode the subpackage encrypted by the previous ones, but since it contains only a third of the original master key as a last resort, no node is able to restore the original data package even partially. According to the protocol, the subpackages will pass through 3–3–3 nodes by the time they get to the exit node. The exit node decodes all three subpackages backwards based on the previous ones and can match the original encrypted data packet and master key with the three subpackages. This will complete the final step of restoring the original data package, which the exit node delivers to the destination server over the open internet. The word onion on behalf of the Tor refers to this structure: the encryption layers of nodes are layered in the same way as the onion layers.

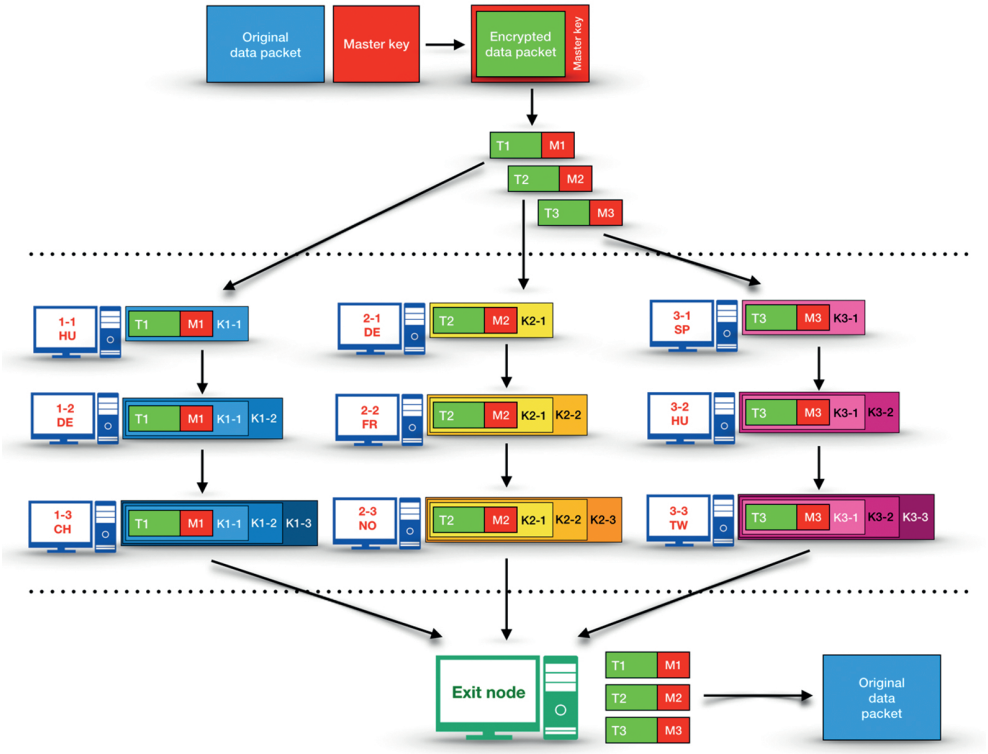

Figure 2. *Tor's encryption model.* [Created by the author.]

Based on the above, beyond exit points, the Tor no longer provides encryption on the Internet, so data traffic between the exit node and the destination server will be open or encrypted depending on the transfer protocol. Therefore, if you need confidentiality, Tor browser should not be used to visit websites which are available on the open Internet and to which the connection is not made via https.

The selection of nodes in each packet was initially random, but according to the Tor protocol specification, the exit node is first determined to make sure it has a connection to the destination. [8]

Based on the above, the logs of a computer serving a web page include only IP addresses for exit points when browsing with Tor Browser instead of the address of the computer that initiated the connection. Therefore, tracing network traffic is available up to this point. Moreover, the addresses of the exit points change from time to time, making it even more difficult to identify. This can be found in the following example: a few lines of a web server log are shown below and each connection was made by different clients. The first items in the log lines are the IP addresses of the computers which download the pages; all three addresses in this example are one of the exit points on the Tor network. [9]

```
198.98.50.112 - - [30/Sep/2019:20:12:26 +0200] "GET / HTTP/1.1" 20…
198.98.50.112 - - [30/Sep/2019:20:12:31 +0200] "GET /favicon.ico H…
109.70.100.29 - - [30/Sep/2019:20:12:38 +0200] "GET /?module=cStat…
109.70.100.29 - - [30/Sep/2019:20:12:39 +0200] "GET /templates/fva…
51.15.106.67  - - [30/Sep/2019:20:12:52 +0200] "GET /?module=cISP&…
51.15.106.67  - - [30/Sep/2019:20:12:53 +0200] "GET /templates/fva…
```

Exit points are located in different parts of the Internet. Therefore, the Tor browser automatically bypasses protections which block network connections by a source IP to ensure that a website is not available from specific countries.[13]

Hidden Services of Tor

Tor allows for hidden services (so-called onion services). These are in most cases websites, file sharing, or chat services whose servers cannot be physically located. [10] Hidden services are based on a more complex mechanism that requires the introduction of new communication elements in addition to the creation of previously presented circuits; along with the three introduction points, a rendezvous point is required. [11]

In the case of this use of the Tor network, the addressing of hidden servers is also different from the public Internet DNS system. [12] In traditional DNS, names are included in a hierarchically distributed database, all elements of which are legally managed by the name owner. In a network that provides anonymity, this type of name resolution cannot be provided due to the operation of the logging mechanisms, so the Tor network provides a special method for addressing servers that do not require DNS servers. The name service

[13] For example, the Pandora music site (www.pandora.com) is not available from Hungary.

provided in this way is similar to that used in traditional DNS but introduces a special ending: ".onion".

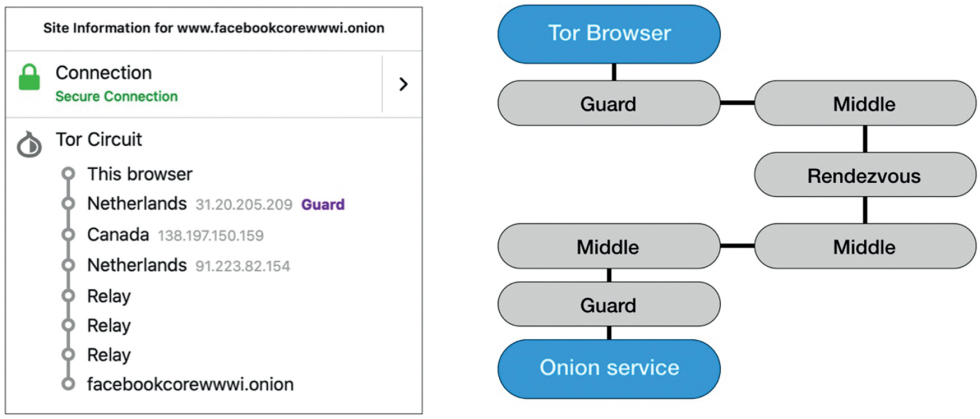

Figure 3. *A path of an Onion service.* [Created by the author.]

The name of the hidden server is formed by an algorithmic path. The name of the server is the Base64 encoded first half of the sha-1 hash of the public key used for communication. This is why the names of servers on the Tor network are not meaningful, easy-to-remember strings. [13, 14] It is possible to create memorable names, but this requires a reverse procedure: the name must be found by trying the above procedure. Finding a key pair for that name requires a lot of computing resources, so most names which were created in this way only refer to the feature in a few characters. According to some calculations, approximately 2.6 million years is required to produce a desired name of 14 characters long, "facebookcorewwwi.onion" used for Facebook is merely the result of a lucky coincidence. [15]

Therefore, IP addressing is only relevant in the lower network layer of the service, and this addressing is no longer relevant to the layers above it, so methods which can work in traditional IP networks are not useable for forensic investigations.

Attack Points

The existence of the Tor network is therefore an advantage on the one hand and a disadvantage for governments on the other hand. PSYOP[14] operations can easily and safely deliver information to targeted areas. Certain types of crimes can be committed without leaving cyberspace. Darknet services play an important role in the communication, financial manoeuvres and fraud management of criminals and terrorist organisations. It is in the interest of repressive regimes to make it impossible to operate, so several measures have been

[14] PSYOP stands for psychological operations, which is based on the information provided to the party to be affected. "In short, PSYOP is the function of the DOD devoted to changing attitudes and behaviour in foreign target audiences; it is frequently described as propaganda outside the military." [16]

taken to achieve this. Bypassing anonymity provided by the Tor network may be a priority for both clients and servers of many national defence and law enforcement organisations. Although, from a technical point of view, Tor is safe, it is possible to successfully attack its users and reveal their identity at several points, as evidenced by several previous examples.

Since most Tor users are not aware of the exact functionality of the technology, there is a good chance that in the long term they will not follow all precautions. The use of the technology keeps them in the misconception that their activities will remain hidden in all circumstances. Human mistakes can be made, and if the authorities are willing to invest a great deal of energy, it allows identification in the long term. Some operators of darknet's largest illegal commercial sites have become identified not because of technological but human error.

One of the best-known drug distribution sites was Silk Road, launched in 2011. In 2013, its operator was identified as a result of a banal error: in a forum post, he used his known darknet name at the same time with his real email address.[15] [17] It has made more than $1 billion in sales over its two-and-a-half-year operation, its operator Ross Ulbrict was sentenced to life in prison in the US.

Faith in the anonymity of cryptocurrencies also proved false: tracking its use made it possible to capture one of darknet's most trafficked child site operators in 2019. [18] This case, if the authorities' claim is accepted, fundamentally calls into question the full confidence in blockchain payments.

Exit nodes are the Achilles heels of the Tor network. If an attacker can take control of such a node due to a possible poor configuration or vulnerability, it can intercept unencrypted data passing through it. It is a good option for authorities wishing to supervise the use of Tor to create or maintain an exit point already set up for attack purposes. This opportunity was demonstrated by Dan Egerstad in 2006, who obtained identifiers and passwords belonging to various embassies, among others the Dalai Lama's office and India's Defence, Research and Development Office. [19, 20] To prevent attacks in this direction, exit points that are unsafe are provided, together with other exit nodes, with BadExit flags and can be filtered on an online map. [21]

To narrow the boundaries of the deepnet and the darknet, search engines use a number of methods that may in some cases prove highly effective. Google, Microsoft and Apple are also trying to do everything they can to collect a lot of data about their customers beyond their browsing habits and geographical location. A huge set of tools are deployed to achieve this goal. In most cases, this is based on the provision of a valuable service to the customer and the requirement of more or less personal data necessary for operation.

Google provides a number of services free of charge, which, by the way, can identify users. They developed their own browser including a sign-in feature. This provides a range of convenient services—storing passwords, organising visited websites—and provides the perfect environment for profiling the user. In addition to the search service, Google's expansion strategy now extends to video streaming (YouTube) for their music service (Google Play Music) and the cloud service for file storage (Google Drive). There are a number of other services that indirectly provide information to implement the profiling

[15] *Source:* https://bitcointalk.org/index.php?action=profile;u=3905;sa=showPosts;start=0

of users. Google stores all the personal activities in their systems which can be traced back later.[16]

In addition to the above, a number of other methods are used to gather as much information as possible. Through the free DNS service,[17] any computer activity that requires name resolution will be known to Google servers. This will inform Google's system about which websites its customers visit as well as which other servers are accessed when using other services. The same service reveals entry points for Google for pages on the deepnet that were previously unknown to them. The free image service lets them analyse millions of images. In these images, the people can be easily identified by facial recognition which, by developing AI, opens up new horizons for them.

The geographical situation of visitors is also known to them. In addition to Google, Apple and Microsoft maintain a database of the hardware addresses of WiFi routers whose geographic location has previously been determined using a device with a GPS receiver. Based on this, they can determine the position of any WiFi device that was once connected by a GPS-enabled mobile phone, but even this is not necessary: Cars which have collected data for Google Street View also have detected and built a database about WiFi routers with their SSIDs[18] and hardware addresses. [22] Moreover, there is no suitable method for avoiding such data collection in real circumstances.

Some traditional hacking tools, such as keyloggers, can easily bypass the protection methods that provide anonymity. DNS also poses vulnerability for anonymous browsers. If a DNS service defines ".onion TLD" in its namespace and registers an onion service address originated from the Tor network, traffic from browsers can be hijacked to a prepared web page outside the Tor network, and that method may lead to the loss of anonymity.

The Tor network could also create a major vulnerability in the protection of IT systems. In addition to the ability to bypass many firewall services, the onion service installed in networks (even a virtual server behind NAT)[19] can maintain a continuous connection to the Tor network. This opens the possibility of access to the protected network without operators enabling it in the firewall configuration. In general practice, a more permissive set of rules is applied to guard protected networks behind firewalls, so launching a hidden service could be the starting point for further attacks. The firewalls don't detect anything from the inward connections because of the contact from behind them.

Knowing the security flaws of individual systems in electronic warfare can be of paramount importance in cyberspace warfare, so they move extremely large resources to achieve a positive position. Software and devices exploiting vulnerabilities are cyber weapons based on which complex cyberattacks can be built. [23] Software enabling vulnerabilities to be exploitable have become commercial products, several companies are involved in their research, acquisition and sale.[20] NSA's XKeyScore system analyses traffic running through more than 700 servers around the world in around 150 key positions during

---

16 *Source:* https://myactivity.google.com/myactivity

17 IP addresses of Google's free name servers are 8.8.8.8 and 8.8.4.4.

18 Service Set Identifier. During the wireless network service, the short name used to identify the device and the service.

19 NAT: Network Address Translation. A commonly used method for hiding networks from others. Behind the NAT device computers do not have a public IP address and cannot be accessed from outside the network.

20 Zerodium offers extremely high fees for a remotely exploitable new vulnerability on the https://zerodium.com/program.html site.

normal Internet usage. Based on the content that runs through it, it creates fingerprints of individual users; in order to activate it one simply needs to visit the Tor or Linux Journal websites. [24] These systems have the means of data collection and triggering capabilities that make it impossible for a person to maintain anonymity for the entire life cycle.

Motion data recorded by GPS-enabled mobile devices can identify their owner without linking them to other databases. Places visited regularly, areas of work, the coordinates of the apartment and their location at a specific time make the person's movement habits precisely identifiable, [25] and compared to the movement of other devices and also his contacts, can pose a serious national security problem.

Based on the examples above, it is clear that internet activity can clearly identify users of the services. It can be said that darknet activity links even a single faulty technical movement when using darknet to one of its other profiles in consideration with the data collected previously. The result of this will be the loss of anonymity.

Application Options

NATO decided at the 2016 Warsaw Summit to declare cyberspace an operational area. [26] The data collection techniques presented so far exemplify the fact that there are a number of possibilities for monitoring and controlling cyberspace, focusing primarily on the hands of the world's leading multinational companies. As cyberspace as an operational area has already been raised, preparations for strategies for it have already begun in several countries, including China and the United States. The question arises as to what cyberspace operations darknet's public services may influence, how they can be used to achieve and maintain cyber superiority, and how they can be used in defensive and offensive operations.

Cyberspace operations are presented in nine main areas that can work in layers of physical, logical, and cyber personality, that make up the structure of cyberspace. [27]

The physical layer is made up of geographical and network elements. Since darknet's operation is based on public internet infrastructure—and its services are provided in the higher tiers—this layer has no significant impact.

Darknet elements are firmly represented in the logical and cyber personality layers. The logical layer includes darknet network infrastructure, protocols that implement anonymity and hiding, and their softwares. On the top, in the cyber personality layer, there are programs which provide the services, e.g. the Tor browser. Darknet services should therefore be taken into account when carrying out cyberspace operations.

In *computer network exploitation,* the aim is to collect as much data as possible and transfer it to processing centres where the data is processed. Darknet's logical infrastructure may play a role in this operation, because it can be used to maintain data connections for which standard firewalls are not an obstacle. Although such a connection does not require significant computing performance, simple IoT devices do not contain enough resources to operate in darknet. On a slightly stronger hardware, with long-term power supply, this connection can be maintained for a longer period of time.

Detection of traffic at a darknet endpoint within a network is not trivial in a network environment that maintains a number of connections with the outside world. Therefore, a minicomputer created to build and maintain a darknet connection is remotely accessible,

opening a backdoor for the attacker. A minicomputer's fast, high-level operating system can run complex softwares. If such a machine is located in a computer network, its darknet traffic is difficult to locate in the case of a carefully configured system and may play an active role in violating any element of the CIA[21] triad.

After the successful installation or placement of such a machine, operational security can be attacked at several points, especially in the field of transmission and network security. The most common of these include—but are not limited to—partial detection of network infrastructure, interception and partial analysis of traffic, collection and transmission of sensitive information in the event of open data transmission, conduct of disruptive activity, services redirecting, deceiving, sending malware to additional network components; but it is also much easier to exploit other security problems from a machine in the internal domain of the network.

Darknet can play an important role in carrying out psychological operations. In doing so, the aim is to provide information to the opposing party that may affect their behaviour, motivations and emotions. PSYOP includes messages of propaganda: white propaganda is the delivery of clearly worded, credible information to the target audience, the purpose of black propaganda is essentially manipulation, the source and content of the information communicated is not real. And grey propaganda seeks to influence the thinking of the target audience by operating with partial truths and time shifts.

Darknet operational capabilities in PSYOP are also to be considered in defence, but may play a role primarily in offensive operations. Because such a server can be created and operated at an extremely low cost, it is therefore highly suitable for creating sources of information that support these operations in such a way that it can only be prevented by serious difficulties concerning the dissemination of information. Hidden services ensure the anonymity of the source of the information, so that the target persons do not have the opportunity to have accurate information about the authenticity of the source and the real entity behind the information. Therefore, this technology is used successfully in grey and black propaganda.

In white propaganda and in the media, darknet's ability to anonymise the target can be used to protect the target, allowing the sender to transmit real information without being detected by authorities.

However, darknet is not generally known and is much more difficult to use. The address of the wanted website is difficult to memorise. Therefore, darknet cannot be effective without education having been organised before it is used, for which other channels should be used.

Analysing Tor Traffic

Tor network statistics are available on Tor Metrics, [28] where the network's operating parameters have been published. Looking back to recent years, there have been several periods in which traffic has increased significantly. There has been a strong increase from September 2013, with the usually 800,000-strong user camp swollen to 5 million over

[21] Confidentiality, integrity and availability.

a short period of time. This was not of social, but of a technical nature. The Mevade/Sefnit botnet, which spread during that period, was communicating on darknet, so the increased user number represented the number of infected machines. In a later version of the botnet, SSH was used, so the load on the Tor network also dropped to normal. Publishing technical enhancements has brought about a similar change: the appearance of the Snowflake plugin for browsers has inspired many users to try it out, which could be seen in Tor Metrics charts for a short period of time.

Monitoring the user number and Tor network load during cyber protection can provide useful information about when a malware appears and when it communicates over the Tor network; monitoring of this could be important for an organisation's IT operators.

Tor usage rate can be measured by network traffic.[22] I could not find any current research publishing the results of such a measurement, so I developed a methodology for this and measured the volume of traffic sent to and from the Tor network for six weeks at Eszterházy Károly University. I evaluated the data by analysing logfiles; during the evaluation, I processed them with shell scripts based on Unix filters. The objectives of the investigation were as follows:

- Description of the amount, nature and volume of traffic coming into the University's network from the Tor network.
- Quantification of the use of the Tor network by university students and staff.
- Detection of the appearance of an onion service or exit point and determination of the detection methodology.
- Comparison of attack traffic from the Tor network and public internet.
- Assessment of the situation revealed in the course of measurements, elaboration of a strategy and drawing of possible conclusions.

I collected the data on which the measurement was based in logfiles. To extend the logging mechanism, it was necessary to change the settings of the university's central routers. Setting up the measurement configuration was based on the fact that the Tor network hides only the user on the one hand and the website you visit on the other, and not the fact of using the Tor network.

Data sources from the Tor network can be clearly identified as this list is made available continuously by network operators in an easy-to-process form.[23] Because exit points can change, its set needs to be updated with a script which runs at least every day. During the measurement, we recorded the IP addresses of source exit nodes, the target computer of each data package, and the target port. The destination port provides information about the service of the university network, e.g. viewing a website or attempting to access a server management interface.

In analysing the nature of traffic, we found that HTTP and SSH traffic dominated as 99% of the darknet traffic is directed at them. This is unexpected given that there are several services known from previous vulnerabilities in the university network. Attacks based on exploiting DNS vulnerabilities belong to the most effective methods, and the RDP protocol

[22] Detection of solutions concerning the previously presented VPN connections is beyond the scope of my investigation.

[23] The list of Tor exit nodes is available on https://check.torproject.org/cgi-bin/TorBulkExitList.py?ip=1.1.1.1 website.

has been a priority in the forecasts for 2019. [29] Despite this, the number of attacks directed to these services from the darknet was minimal.

Protocol	Packets
ssh	600 606
http	505 661
domain	5 252
https	1 748
smtps	166
imaps	108
http-alt	100
smtp	58
netbios-ns	38
submission	34
telnet	22
imap2	20
rdp	18
rdp?	14
ftp	2

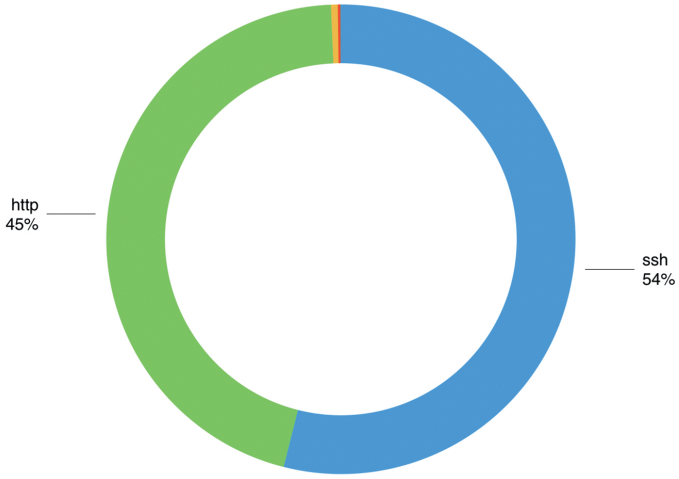

Figure 4. *The protocol distribution of darknet traffic.* [Created by the author.]

According to further measurements, data packets to e-mail softwares were in a similarly low number. The number of spams did not decrease noticeably in recent years, but there is no need to send mail on the darknet. Due to the operation of the SMTP[24] protocol, they can be efficiently distributed on the public Internet and the darknet is not ideal for transmission of large amounts of mail data in a short period of time.

RDP and SSH protocols allow remote logon typically to server computers. SSH is very prevalent in remote management of Unix-based systems, so this connectivity is in most cases thoroughly protected and there is extensive documentation of its methods on the Internet. Thus, from changing the service default port to disabling administrative logins and combining failed login attempts with firewall rules, there are many protection options available. However, it is not expected that a legal request for connections from the darknet will be necessary. These connections are predominantly from softwares that attempt to get valid login information. Darknet infrastructure provides a hide-and-hide service for its runners.

In order to ensure risk-proportionate protection, the number and type of attack attempts from the public Internet direction should be examined and compared with those from the direction of darknet. Because most traffic from the public Internet is legal, the method used to measure darknet traffic cannot be used. The solution is the use of honeypot. This is a computer that shows a real service operation to an attacker by allowing known errors to be exploited or a successful login.[25] Honeypots are important parts of identifying and monitoring the initial activity of new malwares. SSH and HTTP traffic were measured

[24] SMTP is a collection of rules for e-mail posting.
[25] Sshesame is a ssh server that provides the attacker with seemingly successful login.

with a honeypot. The results of the investigation in the given period are shown in the table below:

Table 1. *Comparison of darknet and public Internet traffic for SSH and HTTP protocols*
[Created by the author.]

Protocol	Darknet	Public net
ssh	600,606	2,091,682
http	505,661	200,885

It is important that the traffic data of the public net applied to a single computer (to the honeypot), while attack attempts from the darknet were directed to the entire university network, which includes approximately 1,500 computers. Thus, it can be concluded that during this period the maximum attack traffic from darknet was only a fraction of the number of attacks from the public internet.

Examination of Tor relations initiated from the university also yielded informative results. This was also measured by analysing the traffic of a central router, in which we examined only connections where clients did not embed their Tor traffic into a VPN tunnel. In the latter case, because of the encrypted content, it is not possible to determine the real target of the network traffic. Two methods are available: checking the traffic of its default outbound port, or using the addresses of the guard nodes.

In measuring traffic, it was found that approximately 196 connections were initiated during the investigated period, which came mostly from the author, so we could not report significant darknet activity by the client during the period under consideration.

The appearance of a server providing onion service is rather difficult to identify. According to the protocol, this traffic can be linked to guard node traffic, but by using the VPN solutions already presented, the operator can provide an additional hiding procedure. From the monitoring of guard node traffic and its comparison to other data, gained e.g. from observation of 24-hour traffic, it is likely that such a server will operate. Along similar principles, the internal source of an ongoing VPN connection should also be checked.

Conclusions

Encryption of internet traffic, anonymisation services and public availability of procedures providing encrypted connections without central servers transform the work of national security and law enforcement agencies. Former intelligence data collection tools and electronic equipment used for monitoring and listening are expected to solve previously unknown tasks. Public authorities are expected to be aware of the technologies that criminal circles can use under cover and that ensure hidden communication for them.

Blocking or enabling traffic from the darknet is regulated by the IT security policies or the firewall protection policy of many institutions. Act L of 2013 sets frameworks for state and municipal bodies, to which the 41/2015 Regulation of the Ministry of the Interior is added, providing principles for five types of security departments in line with confidentiality, integrity and availability. Rules for critical infrastructures are defined in

Act CLXVI of 2012. Currently, neither these nor other regulations impose restrictions on darknet traffic, so it is currently up to an organisation to decide whether to filter it.

Attacks from the darknet are different in nature from those coming from the public internet. According to my results, it concerns several services and therefore it does not seem appropriate to filter it separately on the servers – the rules enforced on the public internet are sufficient. On this basis, there is no reason to use serious resources in the examined institution to prevent attacks from the darknet.

It could be a good idea to enable web traffic to reach the original destination of the darknet. If it is assumed that persons belonging to groups relevant from the perspective of national security may appear in the organisation, it is worth activating traffic in this direction before an exceptional event indeed occurs. A change in the level of activity may predict preparations for an act. In the case of public and municipal organisations, especially critical infrastructures, it is expected that Tor servers will not be able to operate in their IT systems. In addition to distributing illegal content, their presence can also help attack protected network elements, so detection of their appearance, continuous monitoring and automation of these organisations is an important task.

References

[1] KEMP, S.: Digital 2019: Internet trends in Q3 2019. *Datareportal*, 2019. https://datareportal.com/reports/digital-2019-internet-trends-in-q3 (Downloaded: 2.10.2019)

[2] DEYAN, G.: How Many Websites Are There In 2020. *techjury*, 2019. https://techjury.net/blog/how-many-websites-are-there/#gref (Downloaded: 25.10.2019)

[3] SANDVIK, R.: The New York Times is Now Available as a Tor Onion Service. *NYT Open*, 2017. https://open.nytimes.com/https-open-nytimes-com-the-new-york-times-as-a-tor-onion-service-e0d0b67b7482 (Downloaded: 11.11.2019)

[4] BBC News launches 'dark web' Tor mirror. *BBC* (online), October 23, 2019. www.bbc.com/news/technology-50150981 (Downloaded: 10.12.2019)

[5] VANDEKERCKHOVE, W.: Freedom of expression as the "broken promise" of whistleblower protection. *La Revue des Droits de L'Homme*, 10 (2016), 1–17. DOI: https://doi.org/10.4000/revdh.2680

[6] KOCH, R.: Here are all the countries where the government is trying to ban VPNs. *ProtonVPN*, 2018. https://protonvpn.com/blog/are-vpns-illegal/ (Downloaded: 3.10.2019)

[7] CHEREPANOV, A.: Fleecing the onion: Darknet shoppers swindled out of bitcoins via trojanized Tor Browser. *We Live Security*, 2019. www.welivesecurity.com/2019/10/18/fleecing-onion-trojanized-tor-browser/ (Downloaded: 25.10.2019)

[8] DINGLEDINE, R. – MATHEWSON, N.: Tor Path Specification. *Github*, 2019. https://github.com/torproject/torspec/blob/master/path-spec.txt (Downloaded: 03.01.2020)

[9] *List of TOR exit nodes.* https://check.torproject.org/cgi-bin/TorBulkExitList.py?ip=1.1.1.1 (Downloaded: 1.10.2019)

[10] *Onionshare.* https://onionshare.org (Downloaded: 20.12.2019)

[11] WINTER, P. – EDMUNDSON, A. – ROBERTS, L. M.- DUTKOWSKA-ZUK, A. – CHETTY, M. – FEAMSTER, N.: *How Do Tor Users Interact with Onion Services?* 2018. https://nymity.ch/onion-services/pdf/sec18-onion-services.pdf (Downloaded: 11.12.2019)

[12] MOCKAPETRIS, P. V. – DUNLAP, K. J.: Development of the Domain Name System. (Originally published in the Proceedings of SIGCOMM '88.) *Computer Communication Review,* 18 4 (1988), 123–133. www.cs.cornell.edu/people/egs/615/mockapetris.pdf (Downloaded: 12.12.2019)
[13] *HiddenServiceNames.* https://trac.torproject.org/projects/tor/wiki/doc/HiddenServiceNames (Downloaded: 20.12.2019)
[14] APPELBAUM, J. – MUFFETT, A.: The ".onion" Special-Use Domain Name. *IETF,* 2015. https://tools.ietf.org/html/rfc7686 (Downloaded: 10.12.2019)
[15] *Tim Taunbert's Blog*. https://timtaubert.de/blog/2014/11/using-the-webcrypto-api-to-generate-onion-names-for-tor-hidden-services/ (Downloaded: 10.12.2019)
[16] COOK, C. – COVEN, D.: What's in a Name? Psychological Operations versus Military Information Support Operations and an Analysis of Organizational Change. Online Exclusive Article. *Military Review,* 3 (2018). www.armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2018-OLE/Mar/PSYOP/ (Downloaded: 04.06.2020)
[17] NORRY, A.: The History of Silk Road: A Tale of Drugs, Extortion & Bitcoin. *Blockonomi,* 2018. https://blockonomi.com/history-of-silk-road/ (Downloaded: 5.10.2019)
[18] VOREACOS, D.: U.S., South Korea Bust Giant Child Porn Site by Following a Bitcoin Trail. *Bloomberg,* 2019. www.bloomberg.com/news/articles/2019-10-16/giant-child-porn-site-is-busted-as-u-s-follows-bitcoin-trail (Downloaded: 25.10.2019)
[19] ZETTER, K.: Tor Researcher Who Exposed Embassy E-mail Passwords Gets Raided by Swedish FBI and CIA. *Wired,* 2007. www.wired.com/2007/11/swedish-researc/ (Downloaded: 1.10.2019)
[20] Shadows in the cloud: Investigating Cyber Espionage 2.0. Joint Report: Information Warfare Monitor – Shadowserver Foundation. *The Citizen Lab,* 2017. https://citizenlab.ca/wp-content/uploads/2017/05/shadows-in-the-cloud.pdf (Downloaded: 04.06.2020)
[21] *TorMap.* https://tormap.void.gr (Downloaded: 1.10.2019)
[22] MAYER, D.: Google explains why Street Views car record Wi-Fi data. *ZDNet,* 2010. www.zdnet.com/article/google-explains-why-street-view-cars-record-wi-fi-data/ (Downloaded: 11.12.2019)
[23] CSERHÁTI A.: A Stuxnet vírus és az iráni atomprogram. *Fizikai Szemle,* 61 5 (2011), 150–155. http://fizikaiszemle.hu/archivum/fsz1105/cserhati1105.html (Downloaded: 10.12.2019)
[24] TUCKER, P.: If You Do This, the NSA Will Spy on You. *Defense One,* 2014. www.defenseone.com/technology/2014/07/if-you-do-nsa-will-spy-you/88054/ (Downloaded: 6.12.2019)
[25] JOHNSTON, A.: Bradley Cooper's taxi ride: a lesson in privacy risk. *SalingerPrivacy,* 2015. www.salingerprivacy.com.au/2015/04/19/bradley-coopers-taxi-ride-a-lesson-in-privacy-risk/ (Downloaded: 02.01.2020)
[26] SIPOSNÉ KECSKEMÉTHY K.: NATO-csúcstalálkozó az elrettentés és a védelem jegyében (Varsó, 2016. július 8–9.). *Hadtudomány,* 27 1–2 (2017), 114–126.
[27] HAIG Zs.: *Információs műveletek a kibertérben*. Budapest, Dialóg Campus, 2018.
[28] *TOR Metrics Portal.* https://metrics.torproject.org (Downloaded: 01.10.2019)
[29] *PandaLabs Annual Report,* 2018. https://partnernews.pandasecurity.com/uk/src/uploads/2018/12/PandaLabs-2018_Annual_Report-uk.pdf (Downloaded: 01.01.2020)